3. The general attribute-based access control system as recited in claim 2, wherein the access decision sub-module comprises software configured for receiving requests for decisions from the policy enforcement sub-module of the client module, determining whether to grant or deny access based on the configuration of the access control database, and returning the decision to the policy enforcement sub-module of the client module.

4. The general attribute-based access control system as recited in claim 3, wherein the resource servers, the access control database, the client modules, and the server modules are included within one or more computer systems.

5. The general attribute-based access control system as recited in claim 4, wherein an assignment between entities can only be established between any of the users and any of the user attributes, any of the user attributes and any other of the user attributes, any of the user attributes and any of the policy classes, any first object attribute and any second object attribute where the second object attribute is not an object, any of the object attributes and any of the policy classes, any of the user attributes and any of the operations, or any set of the operations and any of the object attributes, such that no chain of assignments exists that starts and ends with the same entity, wherein the assignment relations are established by the execution of administrative operations, wherein any user, any user attribute, or any object attribute belongs to any policy class and any policy class contains any user, any user attribute, or any object attribute if there exists a chain of assignments that starts with the user, the user attribute, or the object attribute and ends with the policy class, wherein any user has any user attribute if there exists a chain of assignments that starts with the user and ends with the user attribute; and wherein any object has any object attribute if there exists a chain of assignments that starts with the object and ends with the object attribute.

6. The general attribute-based access control system as recited in claim 5, wherein the permission is any triple including any user, any of the operations, and any of the objects, derived from assignments, where for each of the policy classes containing the object, the user has a user attribute belonging to the policy class, and the object has an object attribute belonging to the policy class, and there is a set of the operations that contains the operation such that the user attribute is assigned to the set of the operations and the set of the operations is assigned to the object attribute.

7. The general attribute-based access control system as recited in claim 6, wherein any pair comprising any of the operations and any of the objects is a capability of any user if the triple including the user, the operation, and the object is one of the permissions.

8. The general attribute-based access control system as recited in claim 7, wherein the prohibition relations include user deny relations where each user deny relation is any triple comprising any of the users, any set of the operations, and any set of the objects, and process deny relations where each process deny relation is any triple comprising a process identifier, any set of the operations, and any set of the objects.

9. The general attribute-based access control system as recited in claim 8, wherein the access decision sub-module is configured with a reference mediation function that determines whether to grant or deny any access request that includes any operation and any object, the access request being issued by any process identified by a unique process identifier and being executed on behalf of a unique user, the reference mediation function grants the access request if the triple including the user, the operation, and the object is one of the permissions, and if no user-deny relation exists that includes the user, any set of the operations, and any set of the objects, where the operation included in the access request is included in the set of the operations of the user-deny relation and the object included in the access request is included in the set of the objects of the user-deny relation, and if no process-deny relation exists that includes the process identifier, any set of the operations, and any set of the objects, where the operation included in the access request is included in the set of the operations of the process-deny relation and the object included in the access request is included in the set of the objects of the process-deny relation, otherwise the reference mediation sub-module denies the access request.

10. The general attribute-based access control system as recited in claim 9, wherein each of the obligation relations is any pair that includes an event pattern and a response, where the response includes a sequence of administrative operations applied to prescribed elements of the basic sets and the basic relations, and the event pattern specifies conditions that cause the event processing sub-module to execute the administrative operations on the prescribed elements when a successful execution of any operation on any object meets the conditions.

11. The general attribute-based access control system as recited in claim 1, wherein the data of the basic data sets that corresponds to the users represents the human users.

12. A general attribute-based access control method, comprising:

selecting an attribute-based access control policy for specification and enforcement;

establishing a configuration of basic data sets in an access control database for the selected attribute-based access policy through execution of predefined administrative operations, the basic data sets including users, user attributes, operations, objects, object attributes, policy classes, and processes, the objects are names for computer-accessible resources to which access by the processes is controlled and which may be stored on a resource server, and each object is also an object attribute, the operations are actions that can be performed on a resource, and the processes are computer programs executed on behalf of any user having a unique identity and that can issue access requests; and

establishing a configuration of basic relations between the basic data sets, the basic relations including assignments, prohibitions, and obligations for the selected attribute-based access policy, through execution of the predefined administrative operations, wherein any assignment between entities can be established only between any user and any user attribute, any user attribute and any other user attribute, any user attribute and any policy class, any first object attribute and any second object attribute where the second object attribute is not one of the objects, any object attribute and any policy class, any user attribute and any set of the operations, or any set of the operations and any object attribute, such that no chain of assignments exists that starts and ends with the same entity, wherein any user, any user attribute, or any object attribute belongs to any policy class and any policy class contains any user, any user attribute, or any object attribute if there exists a chain of assignments that starts with the user or user